Title: Targeted Delivery of Informational Content with Privacy Protection
Inventor: Juels
Serial No. Not yet assigned
Atty Docket No. RSA-044 (7216/66)
Atty/Agent: Ira V. Heffan
Express Mail Mailing Label No. EL750476114US

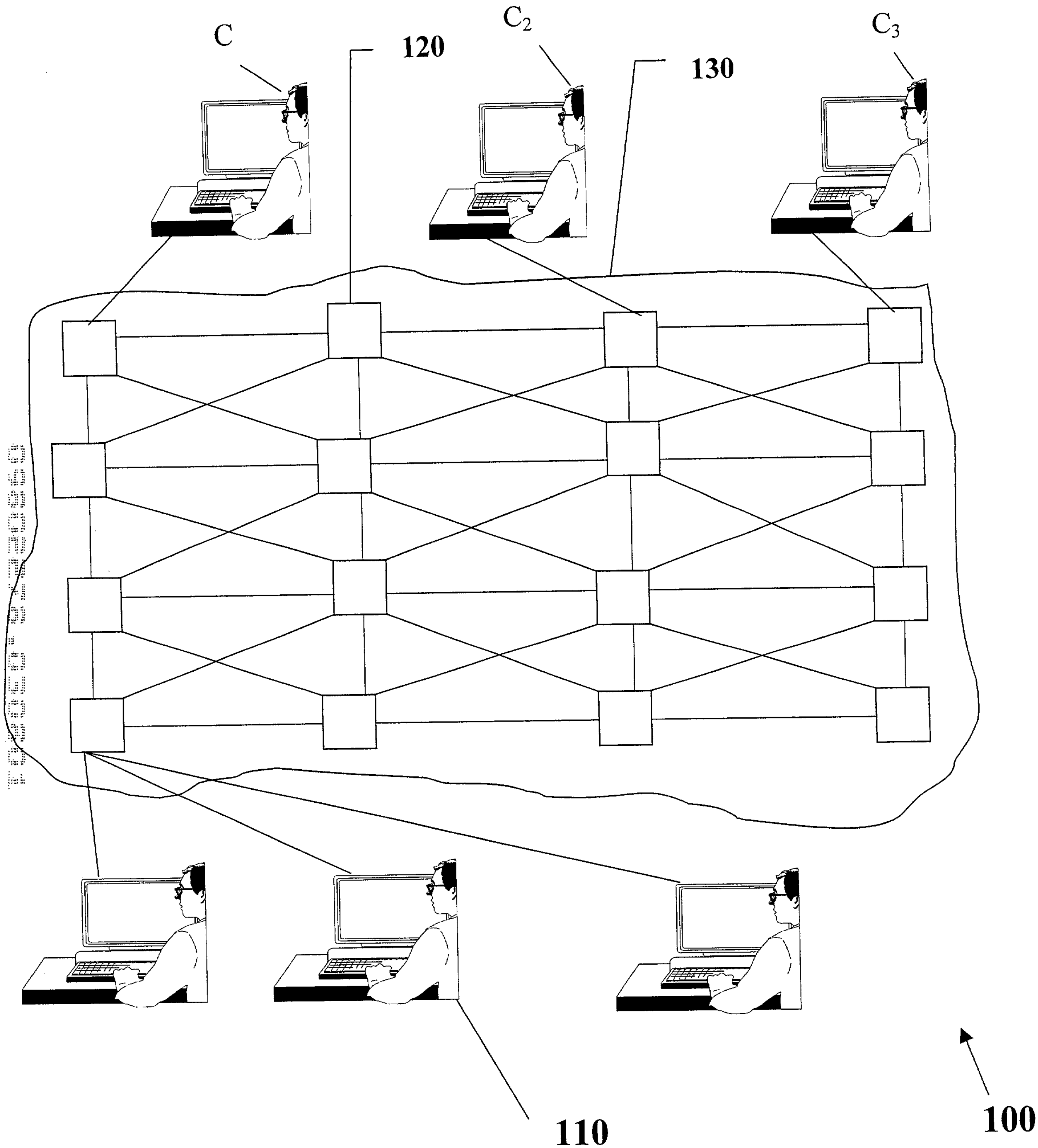

FIGURE 1

Title: Targeted Delivery of Informational Content with Privacy Protection
Inventor: Juels
Serial No. Not yet assigned
Atty Docket No. RSA-044 (7216/66)
Atty/Agent: Ira V. Heffan
Express Mail Mailing Label No. EL750476114US

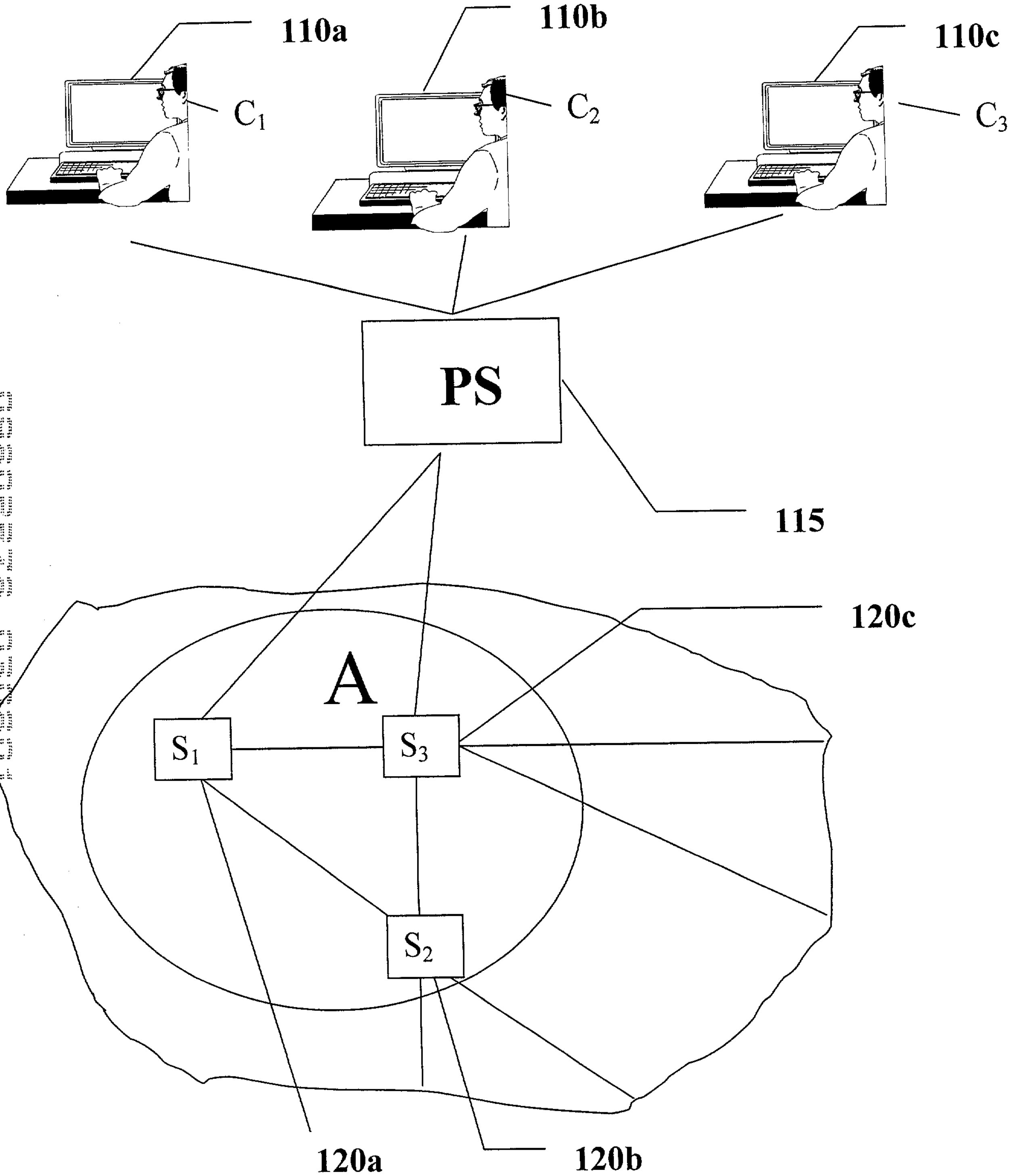

FIGURE 2

Title: Targeted Delivery of Informational Content with Privacy Protection
Inventor: Juels
Serial No. Not yet assigned
Atty Docket No. RSA-044 (7216/66)
Atty/Agent: Ira V. Heffan
Express Mail Mailing Label No. EL750476114US

$C_1, C_2, C_3 \xleftarrow{\quad f \quad} A$ **STEP 31**

C_i computes $r_i = f(P_{Ci})$ **STEP 32**

$C_i \xrightarrow{\quad r_i \quad} A$ **STEP 33**

r_i causes A to select ad_i **STEP 34**

$C_i \xleftarrow{\quad ad_i \quad} A$ **STEP 35**

FIGURE 3

Title: Targeted Delivery of Informational Content with Privacy Protection
Inventor: Juels
Serial No. Not yet assigned
Atty Docket No. RSA-044 (7216/66)
Atty/Agent: Ira V. Heffan
Express Mail Mailing Label No. EL750476114US

$C_1, C_2, C_3 \xleftarrow{f} PS \xleftarrow{f} A$ **STEP 41**

C_1 computes $r_1 = f(P_{C1})$ **STEP 42**
C_2 computes $r_2 = f(P_{C2})$
C_3 computes $r_3 = f(P_{C3})$

$C_1 \xrightarrow{r_1} PS$ **STEP 43**
$C_2 \xrightarrow{r_2} PS$
$C_3 \xrightarrow{r_3} PS$

$PS \xrightarrow{(x_1, r_1)\ (x_2, r_2)\ (x_3, r_3)} A$ **STEP 44**

r_i causes A to select ad_{ri} **STEP 45**

$PS \xleftarrow{(x_1, ad_1)\ (x_2, ad_2)\ (x_3, ad_3)} A$ **STEP 46**

$C_1, C_2, C_3 \xleftarrow{ad_i} PS$ **STEP 47**

FIGURE 4

STEP 51 $C_1, C_2, C_3 \xleftarrow{f} A$

STEP 52 C_1 computes $r_1 = f(P_{C1})$ and encrypts $E_y[r_1]$
C_2 computes $r_2 = f(P_{C2})$ and encrypts $E_y[r_2]$
C_3 computes $r_3 = f(P_{C3})$ and encrypts $E_y[r_3]$

STEP 53
$C_1 \xrightarrow{\{E_y[r_1], x_1\}} BB$
$C_2 \xrightarrow{\{E_y[r_2], x_2\}} BB$
$C_3 \xrightarrow{\{E_y[r_3], x_3\}} BB$

STEP 54 Servers collect $V_1 = \{E_y[r_i], x_i\}_{i=1}^{k}$

STEP 55 Servers mix V_1 by random secret permutation σ_1
to obtain $V_2 = \{r_{\sigma 1}(i), E_y[\sigma_1(i)])\}_{i=1}^{k}$

STEP 56 Servers replace each r_j in V_2 with ad_{rj}
to obtain $V'_2 = \{ad_r, E_y[\sigma_1(i)])\}_{i=1}^{k}$

STEP 57 Servers mix V'_2 by random secret permutation σ_2
to obtain $V_3 = \{(E_y[ad_{\sigma 2(i)}], \sigma_2(i)\}_{i=1}^{k}$

STEP 58 Servers apply quorum controlled asymmetric proxy re-encryption
to obtain $V_4 = (E_{yci}[ad_{ri}], i)_{i=1}^{k}$.

STEP 59 $C_1, C_2, C_3 \xleftarrow{E_{yci}[ad_{ri}]} A$

STEP 60 C_1, C_2, C_3 decrypt $E_{yci}[ad_{ri}]$ to receive ad_{ri}

FIGURE 5

Title: Targeted Delivery of Informational Content with Privacy Protection
Inventor: Juels
Serial No. Not yet assigned
Atty Docket No. RSA-044 (7216/66)
Atty/Agent: Ira V. Heffan
Express Mail Mailing Label No. EL750476114US

STEP 61 $\mathbf{C} \xleftarrow{\quad \mathbf{f} \quad} \mathbf{A}$

STEP 62 **C computes r = f(P) and encrypts $\mathbf{E_y[r]}$**

STEP 63 $\mathbf{C} \xrightarrow{\quad \mathbf{E_y[r_1]} \quad} \mathbf{BB}$

STEP 64 Servers encrypt ad_i to generate $U_1 = \{(j, E_y[ad_j])\}^n_{j=1}$

STEP 65 Servers mix U_1 by random secret permutation σ to obtain $U_2 = (E_y[\sigma(j)], E_y[ad_{\sigma(j)}])^n_{j=1}$

STEP 66 Servers perform a distributed plaintext equality test to find $E_y[j] \sim E_y[r]$ and obtain $U_3 = (E_y[r], E_y[ad_r])$

STEP 67 Servers apply quorum controlled asymmetric proxy re-encryption to obtain $E_{yci}[ad_r]$

STEP 68 $\mathbf{C} \xleftarrow{\quad E_{yci}[ad_r] \quad} \mathbf{A}$

STEP 69 **C** decrypts $E_{yci}[ad_r]$ to receive ad_r

FIGURE 6